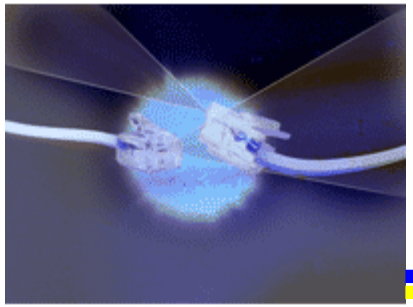
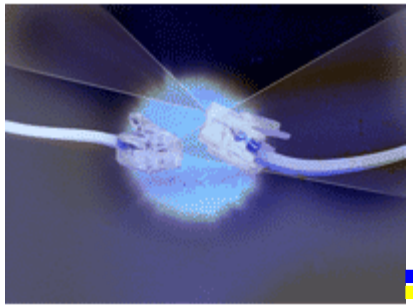


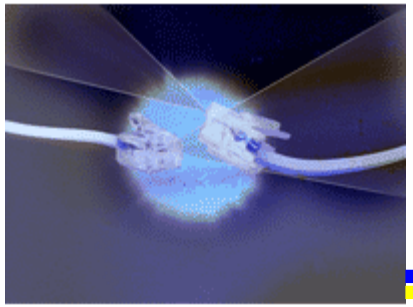
Wireless (802.11)

- IEEE 802.11 – WLAN (Wireless Local Area Network) standard introduced in 1997
  - designed for use in limited areas (building or campus)
- Original standard – up to 2 Mbps using 2.4 GHz radios, using FHSS and DSSS techniques
- Three newer standards:
  - 802.11b (1999) – 11 Mbps using 2.4 GHz, only DSSS
  - 802.11a (1999) – 54 Mbps using 5 GHz, OFDM
  - 802.11g (2002) – 54 Mbps using 2.4 GHz, backward compatible with 802.11b



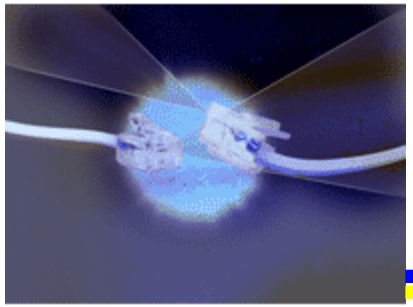
Physical Properties

- Standard provides for three different media
  - Spread spectrum radio – *frequency hopping* (FHSS)
  - Spread spectrum radio – *direct sequence* (DSSS)
  - Diffused infrared
- Spread spectrum intended to spread signal out over broader frequency band than normal
  - Minimize the impact of interference
  - Make eavesdropping harder
  - Make jamming harder



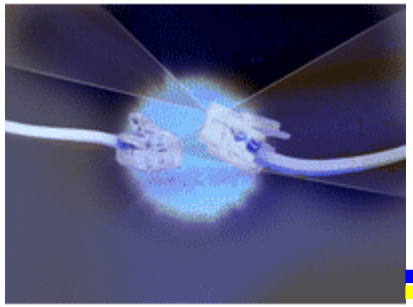
Physical Properties (cont.)

- Original 802.11 - 2.4 GHz frequency band
- Frequency hopping – use pseudo-random code to change carrier frequency to a series of values
  - 802.11 uses 79 1-MHz frequencies
  - Similar to TDM – carrier stays on each frequency for a fixed period of time



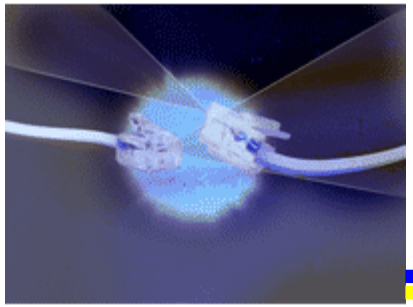
Physical Properties (cont.)

- Direct sequence – XOR each bit of frame with pseudo-random *n*-bit *chipping code*
  - 802.11 uses 11-bit chipping sequence
- Either way, signal looks like noise if receiver doesn't know sequence
- Orthogonal Freq. Division Multiplexing (OFDM)
  - Use multiple carefully spaced carrier frequencies, chosen so they won't interfere
  - Transmit simultaneously on different frequencies – modulate bits onto each carrier



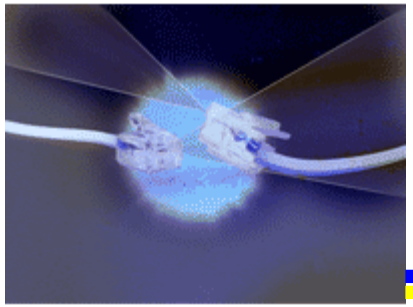
Physical Properties (cont.)

- Diffused infrared – don't need clear line of sight
  - Range only about 10 m, only usable inside a building
- Comparison
  - 802.11a – higher speed, more nodes, less range
  - 802.11b – cheaper, longer range, prone to interference
  - 802.11g – fast, more nodes, longer range, more expensive, prone to interference



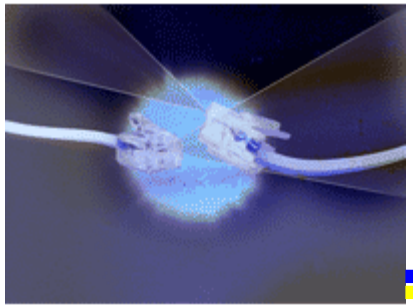
Media Access Control

- Can't use simple CSMA/CD, because not every node might be in range of every other node on network
  - *Hidden node* problem
  - Can cause collisions sender doesn't detect
- Related *exposed node p*roblem
  - Don't need to stop transmitting to all nodes just because you can hear a transmission – destination node might not be in range of the other transmission



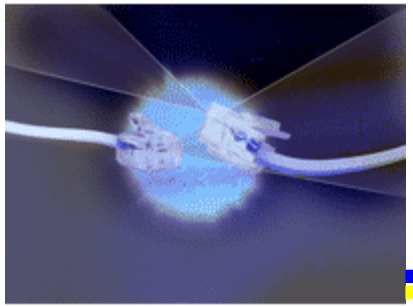
Media Access Control (cont.)

- Alternative is *CSMA/CA* – Carrier Sense Multiple Access with Collision Avoidance
  - Sender and receiver exchange control frames before exchanging data
  - Makes all nearby nodes aware of impending start of transmission
  - Sender sends *RTS* (Request to Send), including length of time to hold medium
  - Receiver sends back *CTS* (Clear to Send) – echoes length field



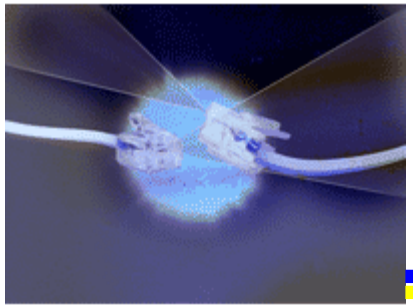
CSMA/CA (cont.)

- Any node that hears CTS cannot transmit for specified length of time
- Any node that sees RTS but not CTS is free to transmit, since it shouldn't interfere with receiver
- Receiver sends ACK after receiving – no node should transmit until it sees ACK
- Senders recognize RTS collision if they don't receive any CTS
  - Use exponential backoff before retransmitting



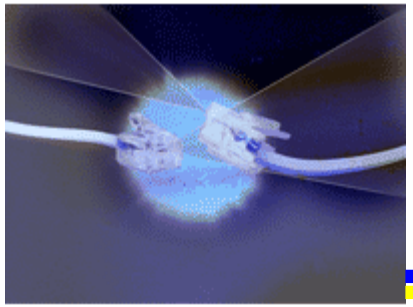
Distribution System

- Nodes can be mobile – set of reachable nodes may change over time
- Standard adds nodes connected to wired network – *Access Points* (APs)
  - Creates set of cells similar to phone system
  - Distribution network runs at OSI layer 2
  - Nodes can communicate directly, but each one associates itself with one AP



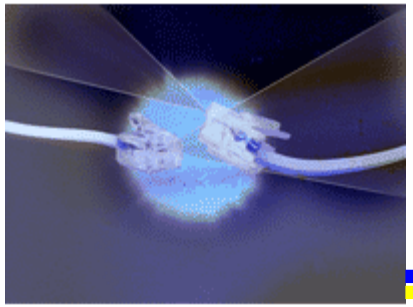
Selecting an AP

- Nodes use *active scanning* process:
  - Send a **Probe** frame (broadcast)
  - All APs in range respond with **Probe Resp.**
  - Node selects one AP and sends it an **Association Request**
  - AP replies with **Association Response**
- APs also support *passive scanning*
  - Send out **Beacon** frames
  - Node can send **Association Request**

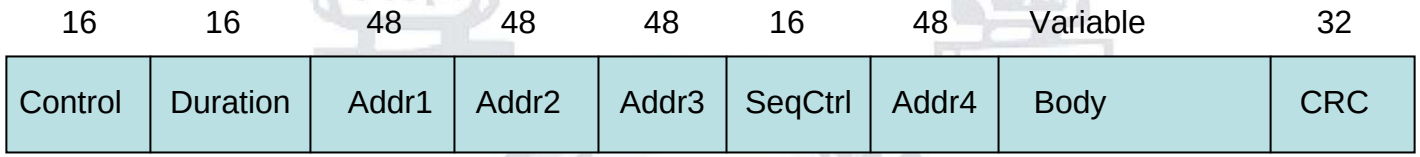


Selecting an AP (cont.)

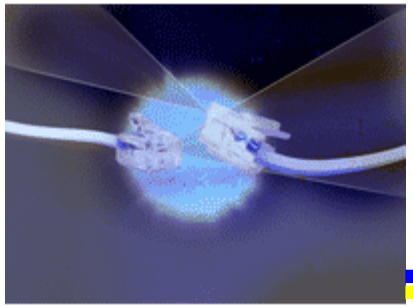
- Scanning must happen each time node joins network, and any time current AP is not satisfactory
  - New AP notifies old AP of change



Frame Format

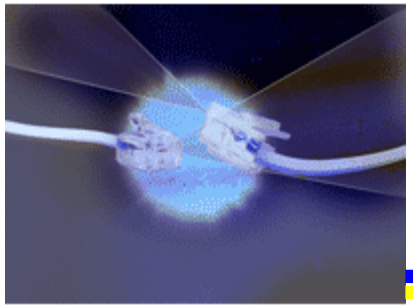


- Up to 2312 bytes (18,496 bits) of data
- Control includes 6-bit **Type** (data, RTS, CTS, or scanning frame) and **ToDS** and **FromDS** bits



Frame Format (cont.)

- Interpretation of addresses depends on **ToDS** and **FromDS** bits
  - Account for possibility that frame was forwarded across distribution system
  - Direct transmission: ToDS == FromDS == 0
    - Addr1 is source, Addr2 is destination
  - ToDS == FromDS == 1 – frame from wireless to AP1 to AP2 back to wireless
    - Addr1 – ultimate dest, Addr2 – immediate src, Addr3 – intermediate dest, Addr4 – original src



Alternatives

- Bluetooth
  - very short range (10 m)
  - relatively low bandwidth (1 Mbps)
  - Connect PDAs or cell phones with PCs
  - Low manufacturing cost